FAQ

FortiClient version 5.4.1/EMS 1.0.1

Fortinet's Advanced Endpoint Protection

FORTINET INTERNAL USE ONLY – Do Not Distribute

1. Product Enhancements

1.1 What's new in version FortiClient 5.4.1 release?

This release aligns FortiClient to Fortinet's integrated architecture offering i.e. Fortinet Security Fabric (FSF) that helps drive *awareness* to every endpoint in each segment of an organization or within an organization as a whole on or off-premises and enables the security operator to respond in real-time to threat containment or non-compliance of endpoint devices.

Namely,

- Endpoint Compliance Enforcement

Introduction of a new tab called "Compliance" on the right in FortiClient's Graphical User Interface (GUI). Should the endpoint be non-compliant, the user can view details in this tab and is offered a button to fix these issues. Once the user has taken the appropriate actions, the endpoint will be authorized for corporate network access.

- Endpoint Telemetry

As part of Security Fabric awareness, endpoint telemetry is sent to FortiGate such as User ID, IP address, MAC address, Avatar, Vulnerabilities, Application information and FortiClient Status. The telemetry data is used for Endpoint Compliance Enforcement as well as responding to threat containment (i.e. endpoint quarantine).

- Vulnerability Scanning with Auto-patching

FortiClient now automates the prevention of known application exploits by keeping all applications on the endpoint up to date.

1.2 What's new in version Enterprise Management Server (EMS) 1.0.1 release?

A new dashboard 'Vulnerability Scan' is added to help the security operator in real-time to identify and respond to endpoints that are running applications that have known vulnerabilities.

1.3 What's changed in FortiClient 5.4.1?

With the release of FortiOS 5.4.1 and FortiClient 5.4.1, management of FortiClient and security profile (AV, App F/W, Vulnerability Scanner, VPN, Web Filter, WAN Opt) is available on EMS only. Net new customers need to license EMS to manage FortiClient and can opt for FortiClient license on the FortiGate to leverage Endpoint Compliance Enforcement, Endpoint Telemetry Network Access Control features. There is a transition plan for existing customers using FortiGate to manage FortiClient to EMS. This is discussed in a detailed FortiClient 5.4.1 license FAQ found here: ***https://fuse.fortinet.com/p/do/sd/topic=370&sid=1856***

1.4 What are the supported upgrade paths to FortiClient v5.4.1?

From version 5.2.4 or later

1.5 What are the supported upgrade paths to EMS v1.0.1?

From version 1.0

1.6 If I want to know more about this release, how can I get more information?

You can stay tuned to monthly email and training updates from the marketing team. You can contact Damien Lim (PMM) or Kunal Marwah (PM) at any time for more information.

2. Product Basics

2.1 What is FortiClient?

FortiClient is a unified endpoint security platform that runs on Windows, Mac, Linux, iOS and Android devices to provide endpoint visibility and control, block known and unknown threats and secure remote access. Although feature set will vary by operating system, core capabilities include anti-malware, application firewall, web filter, vulnerability management, two-factor authentication, remote access and more.

2.2 How effective is FortiClient?

As with other Fortinet threat prevention products, FortiClient is continually measured against leading competitors by independent, real-world testing. Although effectiveness will vary over time, FortiClient is consistently among the top rated products- in 2015 earning AV Comparatives Advanced+ rating, NSS Labs Recommended status in Enterprise Protection Exploit testing with a 98.89% block rate and remaining in the top cluster of Virus Bulletin's Reactive and Proactive testing.

2.3 How is it licensed?

FortiClient is offered as a free download (forticlient.com) which will continually receive security updates. There is an annual charge for Endpoint Compliance and Telemetry feature via FortiClient license for FortiGate. Any organization deploying and managing FortiClients will require Enterprise Management System (EMS) offered as a one, three or five year term license. Refer to the price list for the latest details. For specifics on features between licensed and unlicensed version, please see Table 1 below.

Features	Unlicensed	5.4	5.2
Antivirus (FGL)	✔	✔	✔
Adv Threat Protection (FSA)	-	✔	-
Application Firewall	-	✔	✔
Vulnerability Scanning and Auto-patching	-	✔	✔ (No auto-patching)
Web Filtering	✔	✔	✔
Enhanced Compliance Enforcement	-	✔	✔ (limited telemetry)
IPSec VPN	✔	✔	✔
SSL VPN	✔	✔	✔
Two-Factor Authentication	✔	✔	✔
Windows AD SSO Agent	-	✔	✔
Configuration Provisioning (EMS)	-	✔	✔
Centralized Logging to FAZ/FMR	-	✔	✔
WAN Optimization	✔	✔	✔
Custom Install	-	✔	✔

Table 1. Licensed vs Unlicensed feature comparison

2.4 How can customers manage FortiClient endpoints?

Enterprise Management Server (EMS) installs, manages and provisions FortiClient endpoints.

3. General Questions

3.1 How many clients can be enforced by each FortiGate? Is that a hard limit or a recommendation?

The table below illustrates the maximum endpoints supported by each model. These limits are hard limits enforced by the OS.

Model Range	FortiOS 5.4.1	SKU (current)
FGT/FWF-30 to 90 series	200	FC-10-C0102-151-02-12
FGT-100 to 400 series	600	FC-10-C0106-151-02-12

FGT-500 and above & FGT-VM01 and above	2000	FC-10-C0103-151-02-12
FGT-1000 and above & FGT-VM-04 and above	8000	FC-10-C0104-151-02-12
FGT-3000 and above & FGT-VM08	20000	FC-10-C0105-151-02-12

Table 2. Number of FortiClients supported by FortiGate platform

3.2 How many clients can be managed by EMS? Is that a hard limit or a recommendation?

The "hard-limit" for EMS is 100,000 endpoints. SKU: FC-15-EMS01-158-02-DD. EMS license is per-seat and can be bought in increments of 100 thus provides more flexibility than FortiGate license.

3.3 Would a Fortinet customer need to buy a FortiClient license for FortiGate and one for EMS?

This is dependent on the customer's use-case.
FortiClient license on FortiGate is separate from the one for FortiClient EMS. EMS is mandatory for FortiClient management. A FortiClient license on FortiGate is optional and required only if they want endpoint compliance feature support. Fortinet components **should be positioned** as a solution based on the use-cases below:

3.3.1 Endpoint Installation and Provisioning only: *EMS*
3.3.2 Endpoint Installation and Provisioning with Advance Threat Protection: *EMS* + *FortiSandbox*
3.3.3 Endpoint Installation and Provisioning, and Compliance: *EMS* + *FortiGate*
3.3.4 Endpoint Installation and Provisioning, and Long-term Reporting/Monitoring: *EMS* + *FortiAnalyzer*
3.3.5 Endpoint Installation and Provisioning, and Compliance with Advance Threat
3.3.6 Protection: *EMS* + *FortiGate* + *FortiSandbox*
3.3.7 Endpoint Installation and Provisioning, Compliance, and Long-term Reporting/Monitoring with Advance Threat Protection: *EMS* + *FortiGate* + *FortiSandbox* + *FortiAnalyzer*

3.5 Is there an option for FortiClient to receive signature updates from EMS?

No, currently FortiClient can only get signature updates from FortiManager, FortiGuard Labs or FortiSandbox.

FortiManager can provide signature updates to FortiClient vs FortiClient **(EMS-managed or unmanaged)** getting updates directly from FortiGuard Labs i.e. requires internet access. For customers who operate an air-gapped network or critical infrastructur**e like SCADA/ICS, FortiManager** would be the ideal choice. With the integration of FortiSandbox, FortiClient will receive dynamic signature updates from FortiSandbox to remove malicious object from the compromised endpoint while all other endpoints will be immunized from this threat.

3.6 Which features are required to be installed with FortiClient for FortiGate admin to remotely quarantine the device?

Application Firewall feature is used to remotely quarantine the device from FortiGate or EMS.

3.7 Is FortiAnalyzer required for EMS managed FortiClient for logging & reporting?

Yes, FortiAnalyzer is required. EMS does not provide central logging & reporting.

3.8 How does default gateway MAC address based on-net detection work?

You can now define an on-net ip address subnet range and default gateway MAC addresses to accurately detect when a client in on-net. The subnet must be matched before the gateway MAC address is checked to see if endpoint is on-net.

3.9 Does all members in a FortiGate HA cluster require FortiClient license?

Yes, all members of an HA cluster requires FortiClient license.

3.10 Do I get any FortiClient licenses to try out client management functionality?

Yes. FortiGates with FortiOS 5.4 or EMS include the ability to manage ten clients without any additional license requirement. This helps shorten a POV/POC cycle so take advantage of it!

3.11 Can I use an older 5.x version of FortiClient (e.g. version 5.2) with a newer FortiOS (e.g. 5.4.1 version) or EMS (e.g. version 1.0.1) installation?

Yes, FortiGate running FortiOS 5.4.1 and EMS 1.0.1 is compatible with previous FortiClient 5.x endpoint software. However, keep in mind, EMS was introduced with the release of FortiClient 5.2 thus that is the lowest software version supported. Naturally, benefits of newer features covered in section 2.0 'Product Enhancements' in FortiClient will require an upgrade to version 5.4.1.

3.12 Can I use install the newer FortiClient 5.4.1 and register the license with an older version of FortiGate/FortiOS (e.g. version 5.2)?

No, FortiClient 5.4.1 license will only work with FortiOS 5.4 and above, and EMS 1.0 and above. Customers would need EMS to manage FortiClient if they upgraded to 5.4.1 and used FortiGate to manage previously. An upgrade of FortiOS (to 5.4.1) and/or EMS (to 1.0.1) is highly recommended to support newer enhancements such as endpoint telemetry data that requires an upgrade to these enforcement components. See '1.3 What's changed in FortiClient 5.4.1?' for discussion around FortiClient management transition to EMS.

3.13 Can I upgrade from a FortiClient 5.2 license to a 5.4 license if I want the new features?

Since there are no anticipated changes in licensing structure between version 5.4 and 5.2, you can request for newer licenses as long as the annual support contract is valid and replace existing licenses. Please note there is no upgrade SKU.

3.14 I only use the VPN features of the client, do I need to upgrade?

IPSec and SSL VPN connection from FortiClient 4.3, 5.0, 5.2 should still work with FortiOS 5.4. However, if customers choose to upgrade to FortiOS 5.4.1, then EMS is required to provision VPN. See '1.3 What's changed in FortiClient 5.4.1?' for discussion around FortiClient management transition to EMS.